

EXHIBIT 1

UNITED STATES DISTRICT COURT

for the
Eastern District of Texas

DEC 12 2023

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

The SUBJECT PREMISES 1039 Echols Drive, Frisco,
TX 75306, as more fully described in Attachment A.

Clerk, U.S. District Court
Eastern District of Texas

Case No. 4:23MJ623

APPLICATION FOR A SEARCH WARRANT

I, Justin M. Woodford a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The SUBJECT PREMISES 1039 Echols Drive, Frisco, TX 75306, as more fully described in Attachment A and incorporated herein by reference.

located in the Eastern District of Texas, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. §§ 371, 1030,
1343, 1956 & 1957

Offense Description
Conspiracy to commit wire fraud, fraud related to computers, wire fraud, laundering of monetary instruments, and engaging in monetary transactions in property derived from specified unlawful activity.

The application is based on these facts:
See Affidavit of SA Justin Woodford, Federal Bureau of Investigation, which is attached hereto and incorporated herein by reference.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Justin M. Woodford, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: December 12, 2023

City and state: Plano, Texas

Judge's signature

Hon. Kimberly C. Priest Johnson, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

IN THE MATTER OF THE SEARCH OF:

1039 Echols Drive, Frisco, TX 75306

Case No. 4:23MJ623

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Justin M. Woodford, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the PREMISES known as 1039 Echols Drive, Frisco, TX 75306 hereinafter the "PREMISES," further described in Attachment A, for the things described in Attachment B. As explained in more detail below, the PREMISES is the home of Feng Chen and Tianqiong Xu, who are the individuals behind a complicated scheme to steal cryptocurrency.
2. I am a Special Agent with the Federal Bureau of Investigation and have been since January 2021. Since becoming a Special Agent, I have been assigned to a Cyber Crime Task Force in Albany, NY. I am responsible for investigating complex criminal computer intrusions and cyber fraud, including fraud involving cryptocurrency. I have experience working ransomware, business email compromise, and cryptocurrency trading platform fraud cases, commonly known as "Pig Butchering". I have received training related to cyber security, open-source intelligence, and reverse malware engineering and have a bachelor's degree in Computer and Information Science. I have participated in the execution of search warrants involving electronic evidence, including searches of email accounts and computers.
3. This affidavit is intended to show only that there is sufficient probable cause for the

requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe violations of Title 18, United States Code, Sections 1030 (fraud and related activity in connection with computers), 1343 (wire fraud), 1956 (laundering of monetary instruments and conspiracy to commit money laundering), 1957 (engaging in monetary transactions in property derived from specified unlawful activity), and 371 (conspiracy to commit wire fraud), have been committed by Feng Chen and Tianqiong Xu, in association with a financial scheme designed to defraud victims of currency, including cryptocurrency (the "Subject Offenses"). There is also probable cause to search the PREMISES described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

PROBABLE CAUSE

Overview

5. Since on or around September of 2021, the United States Secret Service and the Federal Bureau of Investigation (the "Investigating Agencies") have been investigating a fraud scheme being used to steal fiat currency and cryptocurrency from individuals located throughout the United States. The scheme utilizes the social engineering of victims who independently navigate on the Internet to platforms for stock and or cryptocurrency investment advice. While on these platforms, the "threat actors" purporting to be investment experts convince these victims to navigate to specific website URLs where they download fraudulent investment platforms to their electronic devices. The fraudulent investment platforms appear to be legitimate cryptocurrency exchanges where the victims can log in and see their investments grow. However, as soon as the victims send their cryptocurrency, the funds begin making their way through a complex laundering scheme. Since at least February 2021, victims of the scheme have been convinced to

transfer custody of their cryptocurrency and/or fiat currency to the Target Subjects under the guise of customer deposits to these cryptocurrency exchanges. The victims later discovered they were unable to withdraw funds they deposited to their accounts, and in some cases, they were extorted for more cryptocurrency or fiat currency when attempting to withdraw.

The Cryptocurrency Investment Scheme

Victim-1

6. On or around September 10, 2021, a victim of the fraud scheme, "Victim-1", was interviewed by the Investigating Agencies. Victim-1, a resident of Vermont, had been defrauded of cryptocurrency valued at over \$600,000 in or around July 2021. During the interview and through communications that followed, Victim-1 provided records, chat transcripts, and information pertaining to her victimization. Victim-1 described the following events:

7. Victim-1 was a participant in WeChat groups focused on stock trading. On or around July 12, 2021, Victim-1 received a private message from a member of one of the stock trading groups that she was a part of on WeChat. The messenger identified himself as "Adl" and claimed to have extensive experience investing. Victim-1 and Adl communicated extensively about investing and their personal lives. They communicated in Chinese. Adl claimed to be from Baltimore, Maryland, but did not provide Victim-1 with his full name or address. Despite not knowing this information, Victim-1 was convinced by her conversations with Adl that he was knowledgeable about investing and trustworthy.

8. On or around July 16, 2021, Adl suggested that Victim-1 begin investing in cryptocurrency. Adl told Victim-1 that he could guide her in getting started. Adl instructed Victim-1 to open a Coinbase account. He then instructed Victim-1 to fund her Coinbase account by wiring money from her bank account. Victim-1 initially transferred \$10,000 from her bank

account to her Coinbase account.

9. Adl provided Victim-1 with a link and prompted her to download a cryptocurrency trading application called BBKX DT to her phone. The link that Adl supplied Victim-1 was: <https://down.bstast.net:8466/Y0TH.app>. Victim-1 downloaded the BBKX DT app using the link provided by Adl. Upon downloading the app, Victim-1 used the app to create a BBKX DT account. In doing so, she provided her email address, phone number, and driver's license. Adl guided Victim-1 through the entire process. According to Victim-1, the BBKX DT app looked to be very legitimate. Around the time that Victim-1 was getting started with cryptocurrency trading using the BBKX DT platform, Adl also requested that she communicate with him using Telegram rather than WeChat. Adl stated that the BBKX DT customer service was located on Telegram but did not provide further justification for switching to the platform.

10. After she had created her BBKX DT account, Adl told Victim-1 to purchase USDC tokens (a type of cryptocurrency) using her Coinbase account, and then transfer the USDC tokens to the BBKX DT platform. To transfer the tokens, Victim-1 used a cryptocurrency wallet address that was connected to her BBKX DT account and could be found within the BBKX DT app on her phone. Victim-1 was prompted by Adl to make several more transactions in which she sent cryptocurrency from her Coinbase account to wallet addresses that were associated with her BBKX DT account. For the deposits to be credited to her BBKX DT account, Victim-1 was required to send a screenshot of each deposit transaction to the BBKX DT customer service via Telegram to confirm the transaction. After the screenshot was confirmed by customer service, the updated balance would be reflected in her account on the app.

11. The BBKX DT app offered a variety of cryptocurrency investment products that gave the user the ability to purchase cryptocurrency, maintain a cryptocurrency savings account, and participate in cryptocurrency trading options. Adl encouraged Victim-1 to continue to transfer

money from her bank account to Coinbase, convert it to cryptocurrency, and deposit it into BBKX DT using the app on her phone. Adl guided Victim-1 as she deposited money into the BBKX DT platform over a period of approximately 11 days. When Victim-1 disclosed to Adl that she had an IRA with a balance of \$300,000, Adl explained to her that she could withdraw from the account for 45 days without penalty. Adl encouraged Victim-1 to deposit the IRA savings into a BBKX DT savings account. At Adl's direction, Victim-1 withdrew the \$300,000 from her IRA and deposited it into BBKX DT. During the period in which she was funding the BBKX DT account at the direction of Adl, Victim-1 believed she was making a profit based on what she was viewing on the BBKX DT app. At one point, Adl told Victim-1 that he would lend her \$50,000 to fund her trading through the BBKX DT platform. Adl sent Victim-1 a transaction confirmation for a deposit of \$50,000 worth of cryptocurrency to her account, and Victim-1 saw a credit for that amount in her account through the BBKX DT app.

12. On or around July 27, 2021, after moving all but \$900 of the money in her bank account to the BBKX DT platform, Victim-1 felt uneasy and attempted to withdraw \$20,000 of her funds from BBKX DT using the app. When she was unable to do so, Victim-1 contacted the BBKX DT customer service on Telegram. She was told that there was only a certain window of time during the day in which withdrawals were processed. When she attempted to withdraw funds during the described window, Victim-1 was still unsuccessful. At this point, the BBKX DT customer service told Victim-1 that there was unusual activity with her account. She was asked to provide additional verification information to customer service at an email address that they provided, including a copy of her driver's license and proof of citizenship. Victim-1 sent most of the requested information and demanded that she be allowed to withdraw her funds. Customer service told Victim-1 that it would take one to three days to conduct an audit of her account. Victim-1 was then told by customer service that she would need to pay a "pledge

deposit” equivalent to 20% of her total BBKX DT account balance to withdraw any funds. Victim-1 was told that her account would be frozen if she failed to pay the required deposit. At that time, Victim-1’s account balance was 622,841 USDT. On or around August 5, 2021, Victim-1 was informed that her BBKX DT account had been frozen, and she lost access to her cryptocurrency.

Victim-2

13. “Victim-2” was interviewed by the Investigating Agencies on or around November 11, 2021. Victim-2 also provided supporting documents to the Investigating Agencies related to her victimization in the fraud scheme. Victim-2, a resident of Michigan, reported being defrauded of cryptocurrency valued at approximately \$179,880.65 U.S. dollars between around March 2021 to around June 2021. In her interview and through associated documents that she provided, Victim-2 described the following events:

14. Around early March of 2021, Victim-2 was approached by an individual named Hao Li, who said he was from Hamburg, Germany, on the communication platform, Discord. Victim-2 was in a Discord channel for stocks and Li was also in the same channel. Victim-2 and Li eventually began exchanging private direct messages on Discord. They would discuss stocks, investments and cryptocurrency. Li seemed knowledgeable about investing. Victim-2 suggested that Li continue talking with her on WeChat. At some point, Li requested they continue talking on Telegram. Li claimed it would be easier to communicate there through direct messages.

15. Through Discord, WeChat, and Telegram Li convinced Victim-2 to invest in the cryptocurrency trading platform called BNB DT. Li sent Victim-2 a link to download the BNB DT app. Victim-2 described the BNB DT platform as having an options trading feature for cryptocurrency that was like options trading for stocks. Victim-2 added the platform had a feature for cryptocurrency lending with good interest rates for depositing Ethereum (“ETH”) and

Bitcoin ("BTC"). The platform also had its own cryptocurrency coin called BNT that Victim-2 traded.

16. The BNB DT platform required Victim-2 to set up an account using the app. This required Victim-2 to provide a passport number and a picture of the passport. Victim-2 supplied these items and created a username and password for access to the account. In addition to the app, there was a website that used the same login credentials as the app.

17. Around May of 2021, Victim-2 had trouble logging into the BNB DT app. Victim-2 went to the BNB DT website and utilized the customer service chat functionality built into the webpage. A response from customer service came to Victim-2's email from bnb@bnb-dt.on.crisp.email. Li informed Victim-2 that a customer service button exists on the BNB DT website as well. Upon clicking the button, Victim-2 was redirected to a Telegram account for BNB DT customer support. The Telegram customer support account directed Victim-2 to download an update for the BNB DT app. When Victim-2 downloaded the updated app, the app name had changed to BBKX DT. Victim-2 still had issues logging into the app on several occasions following the update.

18. Around March 7, 2021, Victim-2 was able to withdraw some funds from the BNB DT app back to Victim-2's originating Coinbase wallet. Approximately 0.0371 BTC was withdrawn, which was around \$1,891 USD at the time. Around late May of 2021, Victim-2 was unable to further withdraw any funds from the BNB DT platform. Victim-2 again contacted BNB DT customer service about the issues withdrawing funds from the platform. Customer service informed Victim-2 that 10 percent of the total account value would need to be paid to withdraw funds. The explanation provided to Victim-2 was the platform was being investigated, so limitations were being placed on withdrawals. Customer service explained that the payment would need to be wired to BNB DT. Victim-2 negotiated the percentage down to 5 percent of the

total account. Li assisted Victim-2 with the customer service negotiations.

Victim-3

19. "Victim-3" was interviewed by the Investigating Agencies on or around October 28, 2021. Victim-3 also provided supporting documents to the Investigating Agencies related to his victimization in the fraud scheme. Victim-3, a resident of Texas, reported being defrauded of money and cryptocurrency valued at approximately \$833,856 between around April of 2021 to around July of 2021. In his interview, in follow up communications with the Investigating Agencies, and through associated documents that he provided, Victim-3 described the following events:

20. On or around March 29, 2021, Victim-3 was contacted through the Telegram communication platform by an individual named "Aileen". Aileen claimed to reside in the United Kingdom. At the time, Victim-3 considered himself to be a beginner in cryptocurrency. He engaged in various discussions related to investment information on the Telegram, WeChat, and Discord platforms. In his communications with Aileen, Aileen told Victim-3 that she could help him make money investing in cryptocurrency with large and quick profits. Victim-3 communicated with Aileen in Mandarin. Besides the Telegram platform, Victim-3 also communicated with Aileen on WeChat.

21. Aileen introduced Victim-3 to BNB DT and instructed him to download the BNB DT app from a specific website. Aileen told Victim-3 that downloading the app from the website instead of trying to get it from a reputable app store was better because it was free to download from the website. Victim-3 followed Aileen's instruction and downloaded the BNB DT app to his cell phone. After downloading the app to his phone, Victim-3 used the app to create a BNB DT account. To create an account for BNB DT, Victim-3 had to provide copies of his driver's license and passport. Furthermore, Victim-3 was told that he needed to set up multi-factor

authentication for the account. This required Victim-3 to also send copies of his bank statements and credit card statements, which he did.

22. On or around April 8, 2021, Victim-3 began depositing cryptocurrency to the BNB DT platform. To fund the BNB DT platform, Victim-3 followed Aileen's instruction, transferring money to his Coinbase account, and then depositing the funds as several different types of cryptocurrencies to wallet addresses that were provided through the BNB DT platform.

23. Victim-3 reported that he would frequently be unable to open the BNB DT app on his phone. When he could not open the app, Victim-3 would contact the BNB DT customer service on Telegram. To reach customer service, Victim-3 sometimes looked them up on the Telegram platform. Other times, he contacted them by clicking on a button that was available within the app. After contacting the BNB DT customer service, they would provide Victim-3 with a link to download a new, updated version of the app. In or around July of 2021, when the BNB DT platform stopped working for Victim-3, the BNB DT customer service on Telegram provided him with a link to download the BBKX DT app. After downloading the BBKX DT app, Victim-3 continued funding the platform in the same way that he had funded BNB DT, utilizing the same account that he had used with the BNB DT app. Victim-3 was not given any information as to why the platform suddenly changed from BNB DT to BBKX DT.

24. At the same time that Victim-3 was communicating with Aileen, he was also communicating with a person named Helen. Helen approached Victim-3 on the Discord communication platform. Victim-3 and Helen continued their communications on the Telegram platform because Helen said it was more convenient to use Telegram than Discord. They communicated in Mandarin. Helen provided Victim-3 with another link to download a cryptocurrency trading app called BFEX. The link provided was <https://www.bf-ex.com/download>. Upon clicking the link, Victim-3 was redirected to <https://down.timcoh.com>.

This website had the appearance of the Apple App Store and a download page for the installation of the BFEX app. An iOS pop-up appeared with the prompt, "This website is trying to download a configuration profile. Do you want to allow this?" and the options, "Ignore" and "Allow". Helen instructed Victim-3 to allow the configuration profile. The downloaded configuration profile was called "BFEX". Victim-3 followed Helen's instructions to install the BFEX app on his phone, using an invitation code provided by Helen to finish the installation. On or around April 3, 2021, shortly before beginning to use the BNB DT app, Victim-3 began using the BFEX app. While Victim-3 utilized a separate account with the BFEX app, he stated that the BFEX app looked very similar to the BNB DT and BBKX DT apps.

25. From on or around April 8, 2021, to on or around July 14, 2021, Victim-3 reported depositing cryptocurrency valued at \$483,856 to the BNB DT, BBKX DT, and BFEX platforms. Furthermore, Victim-3 also made a wire transfer of \$350,000 from his savings account to a JPMorgan Chase bank account that was provided by the BNB DT customer service on Telegram. After making this deposit, 350,000 USDT appeared in the BNB DT app as a credit to Victim-3's account. For every deposit that Victim-3 made to the BNB DT, BBKX DT, and BFEX platforms, he was required to provide a screenshot to the platform customer service verifying the deposit. For BNB DT and BBKX DT, he did this using the app. For BFEX, he provided the information to customer service using Telegram. While Victim-3 was making his deposits to the various trading apps, he believed that he was making a large profit through his use of the platforms.

26. During the time that Victim-3 used the BNB DT, BBKX DT, and BFEX platforms, he was only able to make small withdrawals from the platforms at very limited times. He was successful in making seven withdrawals from the platforms; however, he also had several

withdrawals that were rejected for various reasons. On multiple occasions, Victim-3 was required to pay a fee to make a withdrawal. On the last withdrawal that Victim-3 attempted to make he was told by the BBKX DT customer service that he could not make the withdrawal until the platform had finished updating. Then, Victim-3 was told that he needed to make a tax payment for the profits he had earned prior to withdrawing the money. Victim-3 made this payment and again attempted to withdraw money from his account. At that point, Victim-3 was told that he needed to make an even larger withdrawal payment first. He was then told he needed to make an insurance payment before he could withdraw funds. Victim-3 was never able to make his final withdrawal as he was given a reason as to why he could not withdraw his funds every time he attempted to. On or around early August 2021, Victim-3 was told by customer service that his accounts had been frozen. While he was still able to open the BBKX DT and BFEX apps on his phone at that time, he did not have any access to his funds.

Laundering of the Stolen Cryptocurrency

27. As described above, Victims 1 through 3 were all approached in the spring and summer of 2021 by unknown Chinese-speaking individuals via online communication platforms based on their interest in investing. Each victim was encouraged to download a cryptocurrency trading app from a link that was provided to them. The victims downloaded the apps named BNB DT, BBKX DT, and BFEX using the links they were provided rather than through an app store such as the Apple App Store or the Google Play Store. Some of the same download links were provided to multiple victims. For example, Victims 1 and 3 received the link, <https://down.bstast.net:8466/Y0TH.app>. Additionally, Victim 2 was provided the link, <https://down.aliyunjpl.com/Y0TH.app>, which contained the same “Y0TH.app” file, an indicator unique to the identified fraudulent apps.

28. Each victim was encouraged to invest using the cryptocurrency trading platforms they

had downloaded. The victims were provided wallet deposit addresses through the apps. Unlike with typical centralized custodial cryptocurrency exchanges, the victims were not provided with deposit addresses unique to their accounts. During the time that Victims 1 through 3 were investing using the BNB DT, BBKX DT, and BFEX platforms, each were led to believe through their engagement with the platforms that they were profiting from their investments made using the apps. Furthermore, Victims 1 and 3 each reported having to verify each deposit they made to the apps by providing the platform customer service with a screenshot containing details of the deposit. This suggests that the victims' balances seen on the apps were being manually updated by the entity controlling the platforms.

29. Victims 1 through 3 reported losing access to the funds they invested using the BNB DT, BBKX DT, and BFEX platforms. Each victim lost access to the apps and their funds around the time they fell out of communication with the person who had originally introduced them to the platform and guided their use of the apps, which suggests that these people were involved in the fraud. Additionally, Victims 1 through 3 described having been told by the platform customer service that they were required to deposit additional funds to withdraw their cryptocurrency from the platforms in a manner that is not consistent with industry standards and further suggests the occurrence of fraud.

30. Multiple victims that were interviewed in connection with the above outlined fraud scheme provided cryptocurrency wallet addresses to which they were convinced to deposit cryptocurrency. Many of the wallet addresses provided by the victims were the same, including two wallet addresses provided by Victims 2 and 3. Through blockchain analysis, victim funds were traced by investigators to a custodial wallet address at Binance - 0x9bb4381f58188bf11da82c7d5bbf7adf1f815030 ("0x9bb"). Records obtained from Binance for the account associated with 0x9bb revealed the email associated with that address was

fchen1024@gmail.com. That same email address was still associated with the Binance account in January of 2023. Additionally, the most recent records of the 0x9bb Binance account obtained by investigators revealed the name Tianqiong Xu as the owner of the account, and Xu's Chinese ID as the know your customer ("KYC") document associated with the account. KYC is an industry standard account verification process. Between 4/30/2021 and 01/02/2023, approximately 918,863 USDT has been deposited to 0x9bb. This is equal to approximately \$918,863 U.S. dollars.

31. As described below, further investigation identified Feng Chen as the owner of the email account fchen1024@gmail.com. Tianqiong Xu was identified as the spouse of Feng Chen.

Feng Chen and Tianqiong Xu Were Responsible for the Scheme

32. Binance records were obtained by investigators in September of 2021 and January of 2023 for the account associated with wallet address 0x9bb, which is also associated with email address fchen1024@gmail.com. The Binance returns revealed a login from a device with a Charter IP address (70.119.101.78) located in Allen, TX and a login from a device with an AT&T IP address (45.21.227.112) located in Frisco, TX. Charter records obtained by investigators in October of 2022 revealed the customer associated with IP address 70.119.101.78 is Feng Chen at 405 Spring Leaf Ct. Allen, TX 75002. AT&T records obtained by investigators in January of 2023 revealed the customer associated with IP address 45.21.227.112 is Feng Chen, 1039 Echols Drive, Frisco, TX 75034, the PREMISES. The investigation determined Feng Chen and Tianqiong Xu lived at 405 Spring Leaf Ct., Allen, TX during the time in which investigators identified victims related to the above referenced fraud scheme, in approximately 2021. Physical surveillance at 1039 Echols Drive, Frisco, TX 75034, the PREMISES, identified Chen and Xu at the location as late as April of 2023. Open-source research along with surveillance at the residence indicates that Chen and Xu moved from 405 Spring Leaf Ct., Allen,

TX, to the PREMISES in approximately November of 2022.

33. On 11/23/2021, I executed a search warrant for data stored at Google related to email account fchen1024@gmail.com. As described in more detail below, analysis of the data returned from the search warrant revealed evidence of Feng Chen and Tianqiong Xu's involvement in the scheme.

Google Search Terms

34. I reviewed the Google search warrant return and found many Google web browsing searches made by the account, fchen1024@gmail.com, that were related to the criminal scheme in various ways. The Google searches occurred during the time frame in which victims reported to investigators they had been victimized, as well as shortly before the first identified victim was defrauded. Some examples of these searches appear below.

Crisp Chat

35. On 1/22/2021 Chen conducted a Google search for Moduyun Customer Service. The 'Domain Name System' 'Mail Exchange' (DNS MX) record for both bnb-dt.pro and bf-ex.com was mx01.dm.moduyun.com. The domains, bnb-dt.pro and bf-ex.com were both reported to the FBI by victims of the scheme as fraudulent platforms. A DNS MX record directs email to a mail server and indicates how email messages are routed. A review of the website moduyun.com revealed Moduyun is a China based company that provides online infrastructure and applications. A DNS MX record of mx01.dm.moduyun.com indicates the use of email services purchased from Moduyun. Furthermore, a review of DNS records for the domain mx01.dm.moduyun.com indicated that several other domains that are fraudulent cryptocurrency platforms have this as the MX record.

36. On 2/19/2021, Chen searched for "crisp chat app" and then visited <https://crisp.chat/en/apps>. Victims described to investigators having clicked on a "Customer

Service Button” on the fraudulent cryptocurrency applications they had used. The customer service buttons generated a chatbox which victims used to communicate with the app’s “Customer Service”. Following communication with Customer Service, victims reported receiving an email from the domain “crisp.email”. The email victims received provided a link to a Telegram channel for app “Customer Support”. When the applications that victims were using experienced issues and stopped working, it was from the Telegram channels that victims reported having downloaded app “updates”. Victims also reported communicating with Customer Support on these Telegram channels when attempting to withdraw their funds from the apps. Based on the statements from the victims, it is apparent that each of the fraudulent apps utilized a plugin (a software component that adds a specific feature to an existing computer program) from the company Crisp Chat.

37. On 3/15/2021, Chen received an email containing a chat transcript from transcripts@mail.support.crisp.chat. The transcript contained a conversation between Chen and a Crisp Chat support employee. Chen stated that he has been using the Crisp Chat chatbox on several of his websites for months, but the product had stopped working. The Crisp Chat support employee asked Chen for a website URL that was utilizing the chatbox that was experiencing the issue. Chen supplied the employee with the following URL, “<https://www.bf-ex.com/h5/#/pages/help/center/center>”. Victim-3 reported to investigators that the domain bf-ex.com was the domain for the fraudulent app. Victim-2 reported having received on 3/22/2021 chat transcripts by email from transcripts@bnb-dt.on.crisp.email, which was shortly after Chen contacted Crisp Chat customer service. Victim-2 reported being directed to “<https://bnbdt.pro/h5/#/pages/index/index>” to access the BNB-DT platform. It was on this platform that Victim-2 contacted customer service by clicking on a chat button. This button pulled up a chatbox to chat with BNB-DT customer service. This chatbox was provided by Crisp

Chat. The customer service representative directed Victim-2 to navigate to “https://t.me/BNBDT006”. This URL routed Victim-2 to a Telegram chat to continue communications. The chat transcript format provided by Victim-2 is identical to the chat transcript in Chen’s email.

Searches related to Cryptocurrency Web Application Development

38. On 2/2/2021, Chen searched for “html5 app” and visited the step-by-step guide to publishing an HTML5 mobile application. Web links reported by the victims contained h5 in the URL. H5 is a reference to HTML 5 technologies. HTML 5 allows for the use of web applications to open and be viewed cleanly within a chat application.

39. On 4/29/2021, Chen searched “bnbdt交易所” (bnbdt exchange). On 5/8/2021, Chen searched “BFEX交易所” (bfex exchange). On 5/14/2021, Chen visited “https://bnb-dt.com”. These are only a few examples of numerous searches related to the fraud domains that Chen conducted between 4/29/2021 and 5/14/2021.

40. On 1/25/2021, Chen searched for “crypto invoice generator” and then visited a Reddit thread on /r/Bitcoin called Bitcoin Invoice Generator. Chen also visited Cryptoinvoice on 1/25/2021, a website offering tools to generate invoices related to cryptocurrency transactions. Additionally, on 1/25/2021, Chen searched for “crypto usdt invoice generator”. This activity indicates that Chen was researching how to create professional invoices relating to cryptocurrency transactions.

41. On 01/22/2021, Chen visited a GitHub repository for ccxt which is a code library for accessing cryptocurrency exchange api data. Investigators concluded that the fraudulent web applications pulled real data from legitimate cryptocurrency exchanges, specifically the real-time prices of various types of cryptocurrency. Victims could see the prices live on the web application and also double check the prices on real exchanges while observing no difference. In

my training and experience, some fake cryptocurrency is included within the list of prices. These fake cryptocurrencies are used to control the investments and deceive victims into believing they are making large gains.

GoDaddy and CLEX

42. On 2/1/2021, Chen searched “godaddy standard ucc ssl up to 5 unable to add new domain”. Records obtained by investigators showed a purchase through GoDaddy on 1/26/2021 made by Shopper ID 282928706 of “Standard Multiple Domain (UCC) SSL Up to 5 Domains” for \$199.99. Also purchased by Shopper ID 282928706 were the domain name registrations of bf-ex.com on 12/7/2020, bs-ex.com on 2/1/2021, and bnb-dt.com on 2/17/2021. As previously described, Victim-3 provided investigators documentation of communications with Helen. Helen provided Victim-3 with a link to download the BFEX app. The URL provided was <https://www.bf-ex.com/download>. Additionally, on 1/22/2021, Chen received an email to his fchen1024@gmail.com email from noreply@bf-ex.com with the text, “This is a test” in the body of the email. On 2/18/2021, Chen also received an email to his fchen1024@gmail.com email from noreply@bs-ex.com with the subject “Test – Verification Code.” In my training and experience, the administrator of a domain will test the functionality of their infrastructure by sending an email from the domain to their personal email address with a short message, such as “test”.

43. Records show Shopper ID 282028706 is connected to the following billing information: CLEX LTD, 50 Lorong 40 Geylang, Singapore, Singapore 398074 CN. On 10/5/2020, email address, 786196417@qq.com sent emails to fchen1024@gmail.com containing two .PSD (Photoshop Document) files consisting of an infographic describing what CLEX LTD offers. One .PSD file was in English and the other in Chinese. While searching the fchen1024@gmail.com email, I discovered several other emails from 786196417@qq.com

containing personal documents of Chen and his family. The emails had no messages in the bodies, they only contained documents. These documents included a visa application for Tianqiong Xu, Feng Chen's social security card, and images of Feng Chen's diplomas.

44. Victim-3 reported having been provided whitepapers for the investment platforms he was investing in. A whitepaper is common with cryptocurrency projects. They demonstrate to potential investors the purpose and scope of the project. This can persuade the potential investor that the project is legitimate and worth investing in. The whitepapers provided to Victim-3 were for the platforms BNB DT and BFEX. Each whitepaper was identical to the other except for the names and the document metadata. I looked at the metadata of both .PDF documents and noticed most of the BNB DT metadata was erased. The date of creation for the BNB DT whitepaper was listed as 3/7/2021. The BFEX whitepaper metadata listed Tianqiong Xu's name as the Author of the document. The document was created on 9/28/2020 and last modified on 11/27/2020.

Chen and Xu's Background and Employment

45. While searching the fchen1024@gmail.com account, I found documents containing Chen's educational background and professional skills. In 2010, prior to immigrating to the United States, Chen received his Bachelor's Degree in Applied Chemistry at the China University of Geosciences in Wuhan, China. After immigrating to the United States, Chen received his Master's Degree in 2011 in Petroleum Engineering at the University of Wyoming and his Master's Degree in 2015 in Geology at the University of Louisiana at Lafayette. In 2012, while at the University of Wyoming, Chen processed seismic data by writing computer scripts in the python programming language and then designed a more efficient algorithm in the C programming language. Between 2014 and 2015, Chen described engineering various web development projects. Chen describes possessing skills consistent with someone who could design and execute the web application described in this affidavit. For example, Chen writes that

he has two years of experience developing in HTML5 and CSS. Additionally, he describes experience in web application development utilizing ASP.NET MVC, JavaScript/jQuery/AJAX, LINQ, and ASP.NET Webform. In 2015, Chen wrote a paper titled "Study of Channel Morphology and Infill Lithology in the Wilcox Group Central Louisiana Using Seismic Attribute Analysis", a thesis presented to the graduate faculty of the University of Louisiana at Lafayette. Chen currently is employed as a Software Engineer at Justice Benefits Incorporated (JBI) LTD in Texas. On 10/4/2021, Chen provided documents to Tiger Loans for the purchase of a property located at 5080 Cathy Drive, Forney, TX. The documents provided included a FD-1040 Tax Document from 2020, in which Chen reported making \$74,034 a year and also stated his wife, Tianqiong Xu was unemployed.

Chen and Xu's Purchase of the PREMISES

46. On 10/11/2022, the PREMISES was listed as sold with the last listing sale price of \$1,499,000. As of 12/19/2022, Chen and Xu are listed as the property owners of the PREMISES with a mortgage of \$195,350 and a sale price of \$280,500. From 10/3/2022 to 11/16/2022, Xu's Bank of America account received funds totaling approximately \$1,630,000 that were derived from a personal bank account and a cryptocurrency company, both based in China. On 10/3/2022 Xu received a \$490,000 wire to her Bank of America account from Dongxian Zhou's East West Bank Account, Xu's mother-in-law. Dongxian's East West Bank account was funded by a \$238,560 wire on 8/26/2023, and a \$248,500 wire on 9/27/2022 from a Silvergate Bank account registered to Link-Future Tech Company, a cryptocurrency company based in China. On 10/6/2023, Xu received an \$800,000 wire to her Bank of America account from Guowan Chen's East West Bank account, Xu's father-in-law. From 8/11/2022 to 10/4/2022, Guowan's East West Bank account was funded by four wires totaling \$795,200 from the aforementioned Link-Future Tech Silvergate Bank account. On 11/16/2022, Xu received a \$340,000 wire to her Bank of

America account from a Cathay Bank account registered to Dongxian. Dongxian's Cathay Bank account was funded by a \$349,980 wire from Xu's United Overseas Bank Limited account in Singapore on 10/20/2022. The purchase of the PREMISES would not be possible based on Chen's reported income as the sole earner for the family. Additionally, Guowan Chen claims to make 15,000 Chinese Yuan as the owner of a Grocery Store in China, this is approximately \$2,100 USD. Dongxian Zhou claims to be a housewife and does not contribute financially. This amount of income does not support the amount of money being wired to Chen and Xu's Bank of America account.

47. Open-source searches for Silvergate Bank show the bank is heavily associated with the crypto industry. Silvergate Capital reportedly shut down operations and liquidated its bank in March of 2023 following the collapse of FTX exchange, as FTX was a major Silvergate customer. The money being transferred from the aforementioned Silvergate Bank account to Chen's parents demonstrates a strong connection to a cash out from a crypto exchange.

48. Public records also show Feng Chen is still the owner of the residence at 405 Spring Leaf Ct., Allen, TX. A physical surveillance of Feng Chen and Tianqiong Xu conducted on 12/7/2023 observed Xu departing the PREMISES in a white Toyota Sienna bearing Texas license plate SZN-4190 in the morning at approximately 9:27am. Xu was observed departing the PREMISES in a white Porsche Cayenne bearing Texas license plates IYUAN with Chen as a passenger around noon. This physical surveillance and historical physical surveillance demonstrates that Chen and Xu have taken permanent residence at the PREMISES, and Chen appears to work from home. Records show that Chen purchased the white Porsche Cayenne VIN#: WP1AA2AY4PDA10159 and it was registered to Tianqiong Xu on 6/16/2023 and was paid for with a cashier's check for \$99,166.55 to Porsche of Plano. The address on the registration of the Porsche is the PREMISES.

49. It is likely that Chen and Xu used the proceeds from the fraud to purchase the Frisco, Texas home and the Porsche Cayenne. The proceeds from the fraud likely allowed Chen and Xu to purchase the Frisco property without the need to put the Allen, Texas home up for sale. Based on my training and experience, it is possible that Chen and Xu laundered the proceeds of the fraud by funneling them through multiple accounts belonging to Chen's parents, and ultimately purchasing at least one additional property with the funds.

Probable Cause to Search the PREMISES

50. Based on what I have described above, there is probable cause that Chen and Xu are responsible for planning, executing, and profiting from the fruits of this criminal scheme. Chen's Google search history prior to and during the victimizations documented his process in developing the fraudulent web applications. The movement of cryptocurrency from victim accounts to Chen and Xu's Binance account demonstrates their financial connection to the fruits of the crime. The purchase of expensive real estate by no legitimate means further demonstrates how Chen and Xu laundered the funds. Based on my training and experience, account logins to Binance and Google from both 504 Spring Leaf Court, Allen, TX and the PREMISES indicate the planning and development for the scheme was conducted at home. The last known login to Chen and Xu's Binance account used in the scheme from the IP address registered to the PREMISES was in January. This is based on the records requested by investigators at that time. It is likely that Chen and Xu have continued to login to that account and other accounts used in the scheme from the IP address registered to the PREMISES since that time. Xu is in the United States on a student visa and claims to be unemployed. Chen is employed at Justice Benefits Incorporated as a software engineer and based on physical surveillance reports, appears to work from home. In my training and experience, individuals who send and receive cryptocurrency will have either software, or hardware wallets which contain their crypto assets. It is vital to keep

these wallets secure. Therefore, the owner of the wallet will keep the security keys close to their person. A software wallet will be located on one or many phones, or personal computers. Some software wallets can exist as a web browser extension. A wallet can also be represented as a mnemonic device known as a seed phrase. For example, a seed phrase can be made up of twelve unique words that have to be entered in a precise order. The phrase can be entered in the wallet software to fully restore the account. The search of Chen's fchen1024@gmail.com email contained a crypto wallet seed phrase. The creation of a crypto wallet is simple and multiple wallets can be created with ease and be deployed across any device that supports the software. A hardware crypto wallet works in the same way, but utilizes a USB device to store the wallet software. A seed phrase is used in the same way, but in the case of a hardware wallet, the seed phrase must be entered on the USB device, or on software that the USB device is connected to in order to restore the wallet. Since Chen had a seed phrase in his Google account and has experience with cryptocurrency transactions, I would anticipate the presence of both software wallets on cell phones and/or personal computers and also hardware wallets. Chen and Xu also had logins from Chinese IP addresses present on the account logs from both Google and Binance records. In my training and experience, individuals involved in these types of schemes will have cell phones with Chinese SIM cards on their person, or at their home. Chen's parents were known to live with Chen and Xu at the PREMISES, but have since traveled back to China in and around April of 2023. Chen and Xu traveled around that same time back to China, but have since returned to the United States in and around July of 2023. Despite their travel to China, evidence of the scheme will still be present on devices that will likely be located at the PREMISES such as cellphones, laptops, personal computers, portable storage devices, and crypto hardware wallets. These devices can access any and all accounts that were used in the scheme and have used those accounts recently. These devices will contain forensic evidence showing the historical activities

involved in the scheme, as well as notes and documentation. Specifically, Xu utilized devices to write platform whitepapers. These devices left metadata on the documents. Other items like this will likely be located on devices found at the PREMISES. In my training and experience, software and hardware crypto wallets, as well as seed phrases will not be stored far from the owner and will likely be located somewhere secure at their primary residence.

TECHNICAL TERMS

51. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Cryptocurrency or virtual currency is a decentralized, peer-to-peer form of electronic currency. Cryptocurrency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; (2) a unit of account; and/or (3) a store of value, but does not have legal tender status. Unlike “fiat currency,” like the U.S. dollar and the Euro, cryptocurrency is not issued by any jurisdiction and functions only by agreement within the community of users of that currency.
- b. There are many cryptocurrency networks in use. The most popular of these networks include Bitcoin and Ethereum. Each of these networks utilizes its own decentralized public ledger called a blockchain to record all of the transactions associated with that network.
- c. In an Ethereum transaction, Ether (ETH), the native cryptocurrency on the Ethereum blockchain, is sent from one Ethereum address to another. A Ethereum address is somewhat analogous to a bank account number and is represented as a 44-character-long string of letters and numbers beginning with 0x. Each Ethereum address is controlled by a unique corresponding private key, which is a cryptographic equivalent of

a password or pin needed to send funds from an address. Only the holder of an address's private key can authorize any transfers of Ethereum from that address to other Ethereum addresses. Users can operate multiple Ethereum addresses at any given time, with the possibility of using a unique Ethereum address for each transaction.

d. In a Bitcoin transaction, Bitcoin (BTC), the native cryptocurrency on the Bitcoin blockchain, is sent from one or more Bitcoin addresses to one or more Bitcoin addresses. A Bitcoin address is represented by 25 to 35 character-long string of letters and numbers. Bitcoin addresses are also controlled by a private key which allows only the holder to authorize transactions from Bitcoin addresses. Bitcoin users can operate multiple addresses at any given time, with the possibility of using a unique Bitcoin address for each transaction.

e. To transfer Bitcoin or Ethereum to another address, the sender transmits a transaction announcement, which is cryptographically signed with the sender's private key, across the Bitcoin or Ethereum peer-to-peer network, respectively. In general, the amount of cryptocurrency to be sent, the address of the receiving party, and the sender's private key are the only pieces of information needed to complete the transaction; therefore, a Bitcoin or Ethereum address by itself rarely reflects any identifying information. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in the transaction itself. Once the sender's transaction announcement is verified by the network, the transaction is added to the Bitcoin or Ethereum blockchain. The Bitcoin and Ethereum blockchains, respectively, log every Bitcoin and Ethereum address that has ever been involved in a transaction and maintain records of every transaction for each Bitcoin and Ethereum address.

f. The Ethereum network also allows for other items of value, such as tokens, to be

stored and transacted between Ethereum addresses. The rules governing the creation and functionality of these items of value are defined by programs stored on the blockchain called smart contracts. Any Ethereum user can create a smart contract and deploy it on the Ethereum blockchain. Tether USD (USDT) and USD Coin (USDC) are two common tokens that are transacted on the Ethereum blockchain. Transactions involving these tokens are governed by their associated smart contracts. Like all other transactions on the Ethereum blockchain, transactions involving tokens such as USDT and USDC are recorded on the blockchain. These transactions also require some amount of ETH as a blockchain transaction fee.

g. To acquire cryptocurrency, a typical user will purchase it from a cryptocurrency exchange. A cryptocurrency exchange is a business that allows customers to trade cryptocurrencies for other forms of value, such as conventional fiat money (*e.g.*, U.S. dollars, Russian rubles, euros). Exchanges can be brick-and-mortar businesses (exchanging traditional payment methods and virtual currencies) or online businesses (exchanging electronically transferred money and virtual currencies). Cryptocurrency exchanges doing business in the United States are regulated under the Bank Secrecy Act and must collect identifying information of their customers and verify their clients' identities.

h. While the identity of a cryptocurrency address owner is generally anonymous (unless the owner opts to make information about the owner's address publicly available), analysis of the blockchain can often be used to identify the owner of a particular address. Since blockchains serve as searchable public ledgers of every transaction on the corresponding cryptocurrency network, investigators may trace transactions to exchanges. Because those exchanges generally collect identifying

information about their customers, subpoenas or other appropriate legal process submitted to these exchanges can, in some instances, reveal the true identity of an individual responsible for a cryptocurrency transaction.

i. A cryptocurrency wallet is used to store cryptocurrency and can control cryptocurrency addresses associated with multiple blockchains. The wallet interfaces with the blockchain and uses private keys to restrict access to spending the various types of cryptocurrency and tokens stored within the wallet. Cryptocurrency exchanges and users of cryptocurrencies store and transact such funds in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device (“hardware wallet”), downloaded on a PC or laptop (“desktop wallet”), with an Internet-based cloud storage provider (“online wallet”), as a mobile application on a smartphone or tablet (“mobile wallet”), printed private keys (“paper wallet”), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on electronic devices, including computer and mobile devices (*e.g.*, smart phones or tablets), or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency. In addition, paper wallets contain an address and a QR code with the public and private key embedded in the code or may simply consist of a private key printed on a piece of paper. Paper wallet keys are not stored digitally. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). Individuals possessing cryptocurrencies may have safeguards in place to ensure that their cryptocurrencies

become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

j. The most common cryptocurrency exchanges are centralized custodial exchanges, which are controlled by a single entity that holds the private keys to all wallets associated with the exchange. This is similar to a customer depositing funds into a bank where the bank controls access to the vaults and the customer trusts the bank to properly credit their account. A cryptocurrency exchange customer entrusts the cryptocurrency exchange with their deposited cryptocurrency and expects it to be properly credited to their account. Centralized custodial cryptocurrency exchanges typically create one or more unique deposit addresses for each customer account. Because these addresses are associated with a specific account, funds deposited to the addresses can be automatically credited to the associated customer's account.

k. Software that allows a user to perform specific tasks on a computer, such as a word processor or web browser, is called an application. Applications for desktop or laptop computers are typically called desktop applications and those for mobile devices such as tablets and smartphones are typically called mobile apps or simply apps. The most common operating systems for mobile devices are Android and iOS. These two operating systems both offer native platforms, Google Play Store and App Store, respectively, where apps have that passed some level of security and functionality screening can be downloaded.

l. Many cryptocurrency exchanges offer mobile apps so that their services can be easily utilized from mobile devices. Both the Google Play Store and App Store offer apps for well-known cryptocurrency exchanges including Coinbase, Binance, Huobi, FTX, Kraken, and KuCoin.

m. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. There are two versions of IP addresses, IPv4 and IPv6. An IPv4 address is represented by four groups of decimal digits, each in the range 0-255, separated by periods, each group representing 8 bits (e.g., 121.56.97.178). An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

n. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

52. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage

media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

53. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence,

because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on actual inspection of other evidence related to this investigation, I am aware that computer equipment was used to generate, store, and print documents used in the scheme. There is reason to believe that there is a computer system currently located on the PREMISES.

54. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in

use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic

storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary

to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

55. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the PREMISES, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.


56. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

57. Because Chen and Xu's two children live at the PREMISES, and both Chen's mother and father have been known to reside at the PREMISES, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

58. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,


Justin M. Woodford
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on December 12, 2023:



HON. KIMBERLY C. PRIEST JOHNSON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is 1039 Echols Drive, Frisco, TX 75306 and any locked or closed containers and safes therein, any outbuildings or sheds (referred to as the "PREMISES"), the person of Feng Chen and Tianqiong Xu and any and all vehicles owned, leased, rented, or operated by Feng Chen and/or Tianqiong Xu parked on or near the PREMISES at the time of the service of the search warrant.

The PREMISES is more fully described as a large single-family home with a tan stone and brick exterior construction, two large garage buildings connected by a concrete driveway. It is accessed by a front archway under a tan stone spire. The front doorway to enter the PREMISES is an arched wooden and glass door. A photograph of the exterior of the building is below:



ATTACHMENT B

Items to be seized

1. All evidence fruits, and instrumentalities of violations Title 18, United States Code, Sections 1030 (fraud and related activity in connection with computers), 1343 (wire fraud), 1956 (laundering of monetary instruments and conspiracy to commit money laundering), 1957 (engaging in monetary transactions in property derived from specified unlawful activity), and 371 (conspiracy to commit wire fraud) (collectively the "Subject Offenses"), those violations involving Feng Chen and Tianqiong Xu, and others known and unknown, including:

- a. Evidence concerning occupancy or ownership of the PREMISES, including utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, and telephone directories;
 - b. Evidence concerning the identity or location of, and communications with, suspects, coconspirators, and victims of the fraud.
 - c. Records of financial transactions, including banking records;
 - d. Cryptocurrency in any form;
 - e. Cryptocurrency wallets, seed keys/phrases, cryptocurrency transaction records, deposit addresses, or cryptocurrency exchange records;
 - f. Software, white papers, research and development tools, or other information related to the BBKX DT, BNB DT, BFEX applications and platforms;
 - g. IP address and email account records;
 - h. Records related to the purchase of the PREMISES and of a Porsche Cayenne registered to the premises;
 - i. Employment and immigration records, including passports, visas, and records of movement into and out of the United States.
2. Computers, cell phones, tablets, or storage media that may contain any electronically stored information falling within the categories set forth in Sections (1)(a-h), above. In lieu of seizing any such devices this warrant also authorizes the copying of such devices or media for later review. Included within the items to be seized from the PREMISES to facilitate review of such electronic devices are:
- a. Any items or records needed to access the data stored on any seized or copied cellphones, including but not limited to any physical keys, encryption devices, or records of login

credentials, passwords, private encryption keys, or similar information.

b. Any items or records that may facilitate a forensic examination of the cellphones, including any hardware or software manuals or other information concerning the configuration of the seized or copied electronic devices.

c. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied electronic devices.

In searching the electron devices seized pursuant to this warrant, law enforcement personnel are further authorized to seize:

- i. Information and records establishing the identity of the person who used the electronic device;
- ii. Information related to the location of the electronic device and/or its user at the time of the crimes under investigation; and
- iii. Information evidencing the user of the device's state of mind as it relates to the crimes under investigation.

Use of Fingerprints and Face

During the execution of this search warrant, law enforcement personnel are authorized to press the fingers (including thumbs) of anyone present at the PREMISES to the fingerprint sensor of any smartphones or electronic devices seized in connection with this warrant for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. During the execution of this search warrant, law enforcement personnel are authorized to have such individuals remain still and look, with eyes open, at the camera of any smartphones or electronic devices seized in connection with this warrant for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

Review of Electronically Stored Information (“ESI”)

Following seizure of any electronic device and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example: surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); opening or cursorily reading the first few “pages” of such files in order to determine their precise contents; scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files; performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are

intimately related to the subject matter of the investigation; and
reviewing metadata, system information, configuration files, registry data, and any
other information reflecting how, when, and by whom the cellphone was used.

Law enforcement personnel will make reasonable efforts to search only for files,
documents, or other electronically stored information within the categories identified in
Sections (1) and (2) of this Attachment. However, law enforcement personnel are authorized to
conduct a complete review of all the ESI from seized devices or storage media if necessary to
evaluate its contents and to locate all data responsive to the warrant.

As used above, the terms “records” and “information” includes all forms of creation or
storage, including any form of computer or electronic storage (such as hard disks or other media
that can store data); any handmade form (such as writing); any mechanical form (such as printing
or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives,
videotapes, motion pictures, or photocopies).

This warrant authorizes a review of electronic storage media and electronically stored
information seized or copied pursuant to this warrant in order to locate evidence, fruits, and
instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.